ORIGINAL

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
Policies and Rules	)	CC Docket No. 93-292
Concerning Toll Fraud	)	

COMMENTS OF THE INTEREXCHANGE CARRIER INDUSTRY COMMITTEE TOLL FRAUD SUBCOMMITTEE

David P. Jordan
Richard J. Petillo
ICIC-TFS Co-Chairs

Comments Prepared by: Douglas F. Brent
9300 Shelbyville Road
Suite 700
Louisville, Kentucky 40222

DATED: January 14, 1994

SUMMARY

Toll fraud is a nationwide problem which requires comprehensive solutions. The Interexchange Carrier Industry Committee Toll Fraud Subcommittee offers solutions for the types of fraud identified in the Notice of Proposed Rulemaking, as well as for certain problems not discussed in the NPRM.

All carriers, as well as customers, have responsibilities to help detect and prevent toll fraud. In all cases, responsibility for toll theft should be allocated to the party in the best position to prevent it. The Commission should require adoption of certain measures to prevent toll fraud.

In the case of customer premises equipment fraud, including PBX fraud and manipulation of private payphones, the owners of such equipment are in the best position to detect and prevent fraud. IXCs should not be made liable for theft which occurs as a result of the manipulation of CPE.

For fraud related to "0+" and operator assisted calling involving joint use calling cards and LEC-issued line numbers, the Commission should take steps which will encourage LIDB providers to improve existing fraud control features and to develop new ones. The Commission should find the LIDB providers are responsible for the consequences of poor LIDB administration. When LIDB providers are required to have a financial stake in the performance of these databases, they will have incentives to improve their fraud

detection and calling card issuance practices.

Finally, the Commission should take steps to reduce the incidence of subscription fraud, and to eliminate fraud vulnerabilities in LEC optional services such as call forwarding.

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of Policies and Rules Concerning Toll Fraud	)	CC Docket No. 93-292

COMMENTS OF THE INTEREXCHANGE CARRIER
INDUSTRY COMMITTEE TOLL FRAUD SUBCOMMITTEE

The Interexchange Carrier Industry Committee Toll Fraud Subcommittee[1] ("Toll Fraud Subcommittee" or "TFS") files these comments in response to the Commission's December 2, 1993 Notice of Proposed Rulemaking ("NPRM" or "Notice") in the referenced proceeding. The TFS applauds the Commission's decision to consider the nation's serious and growing toll fraud problem through a rulemaking proceeding. The Toll Fraud Subcommittee supports the Commission's attempt to find comprehensive solutions for the fraud problem.

---

[1]The Toll Fraud Subcommittee's primary purpose is to address matters being considered by the Network Operations Forum's Toll Fraud Prevention Committee. However, the TFS was also formed for the purpose of addressing governmental requests and mandates for interexchange industry consensus regarding technical solutions to fraud problems and other non-competitive technical issues related to theft of service and unauthorized network access. Members of the TFS include AT&T, MCI Telecommunications, Sprint Communications Co. L.P., LDDS Communications, Inc., Teltrust Communications Services, Inc., Stentor Alliance, Consolidated Communications Operator Services Inc. and Consolidated Network Inc.

I. BACKGROUND.

The Toll Fraud Subcommittee's comments suggest solutions for the types of fraud identified in the NPRM, as well as for certain fraud problems not specifically discussed in the Notice, including subscription fraud and abuse related to LEC call forwarding, remote call forwarding and three way calling services.

Telecommunications theft occurs as the result of many events, including use of stolen or fraudulently obtained calling card numbers and other access devices, compromised customer premises equipment, subscription fraud, electronic manipulation of cellular phones and use of service without intent to pay for it. All of these thefts result in usage of LEC and IXC networks and toll services. Such thefts increase IXC uncollectibles, and like all thefts, ultimately increase the prices paid by all telephone subscribers.

IXCs can and do help to detect and prevent certain types of toll fraud. They educate their customers about the risks of fraud, and advise customers and employees about the need to protect a account information, calling card numbers and access codes from improper disclosure. IXCs also document and investigate fraud involving their networks, cooperate in investigations, and support tougher criminal statutes for theft of service.

The Toll Fraud Subcommittee supports the concept of allocating responsibility for toll theft to the party in the best position to prevent it. NPRM, ¶ 24. For example, IXCs monitor the usage of their own calling cards and are responsible for the fraud.

However, in many cases, LEC business practices expose IXCs to unnecessary toll fraud risks. As discussed below, some types of toll theft are best prevented by customers.

The Commission can require adoption of certain measures to prevent toll fraud using existing technology. By doing so, and by adopting reasonable liability apportionment principles, the Commission will eliminate the need to establish a Federal Advisory Committee on toll fraud issues. See NPRM, ¶ 13. Establishment of an additional committee is not the best solution; with appropriate incentives, existing industry standards groups can eliminate many of the fraud problems affecting the industry today.

Set forth below are the Toll Fraud Subcommittee's comments regarding specific types of fraud described in the NPRM.

II. PBX FRAUD.

The TFS strongly opposes any proposal to make IXCs liable for fraud caused by unlawful manipulation of any customer premises equipment, including PBXs, voice mail systems, automatic call distributors, and private payphones. There is no reason to depart from the Commission's recent, well-reasoned Chartways decision concerning subscriber responsibility for PBX toll theft. Chartways Technologies, Inc. v. AT&T Communications, 6 FCC Rcd. 2942 (Com. Car. Bur. 1991). In Chartways, the Common Carrier Bureau found the PBX owner had control over ingress and egress from its privately owned switch. Thus, the subscriber was found to be responsible for all calls originating at its PBX. The Bureau's findings were upheld by the Commission. 8 FCC Rcd. 5601 (1993).

As the Commission observes in ¶ 3 of the Notice, control over the use of telecommunications services has increasingly shifted from carriers to individual consumers. When shifts in control occur, shifts in responsibility follow. Chartways is consistent with the general principle that responsibility lies with the party best able to prevent fraud.

Clearly, the PBX owner is in the best position to prevent misuse of its CPE, just as the PBX owner is in the best position to prevent unauthorized access to its other property. In addition, the PBX owner has full control over which PBX features are to be used. Specifically, the Direct Inward Service Access ("DISA") function often implicated in PBX theft cases is an option used at the sole discretion of the PBX owner. PBX owners can disable DISA features, and there are reasonable alternatives to DISA usage, including LEC and IXC calling cards. Moreover, the PBX owner has the option to permit inward access over an 800 number or local lines while restricting the ability of inward callers to select outgoing trunks.

In contrast, IXCs have a duty to complete all messages transmitted from a customer to their networks, and generally have no basis to block calls originating from a PBX. It is virtually impossible for an IXC to distinguish legitimate outbound traffic from traffic occurring as a result of unlawful PBX manipulation. Moreover, outbound traffic may be stimulated by a variety of factors unknowable by the interexchange carrier, including increased business activity, call forwarding to another PBX, and

outbound telemarketing.

PBX owners and their industry groups have often claimed that IXCs have no incentive to help prevent or curtail PBX and other non-card fraud. The difficulty with this claim is that even if an IXC is not liable for charges arising from toll theft, such thefts produce significant uncollectibles for the IXC and result in the imposition of LEC access charges which must be paid regardless of whether the related toll revenue is ever collected. Moreover, scanning and hacking of 800 numbers may create disincentives for business subscribers to use these services, because costs are imposed on the subscriber even when hacking attempts fail to create outbound calls. Clearly, IXCs already have economic incentives to help limit PBX fraud.[2]

In ¶ 24 of the NPRM, the FCC states its tentative conclusion that tariff liability provisions that fail to recognize an obligation by the carrier to warn customers of the risk of using carrier services are unreasonable. The Toll Fraud Subcommittee cannot understand the Commission's tentative conclusion, because a major premise of the Commission's conclusion is incorrect. The risk is not in using carrier services; rather, it is in using a PBX. In any event, warning notices in IXC tariffs would not be the best way to put PBX owners on notice. Rather, such notice could

---

[2]An example of a fraud problem where a carrier may lack sufficient incentives to help its customers is "0+" fraud exacerbated by problems with LIDB. In such cases, the LEC's customer is not the caller, but the IXC validating calls through LIDB. Since there are minimal financial consequences to LECs as a result of LIDB errors, the LIDB providers may not have sufficient incentives to improve LIDB, thereby assisting their IXC customers.

come from PBX manufacturers and distributors and perhaps from local exchange carriers who offer the trunks needed to interconnect a PBX with the switched network.

In ¶ 25 of the Notice, the Commission asks for comments on whether to apportion the cost of CPE-based fraud based upon who is in the best position to avoid, detect, warn of, or control the fraud. As discussed above, the TFS supports an approach where the liability is based upon control. In the case of PBX fraud, all of these factors point to the CPE owner. Although CPE manufacturers arguably are in the best position to warn of the potential for toll theft, it is the CPE owners who have the ability to secure ingress and egress from their equipment.

The Commission also asks whether residential ratepayers would bear the burden of business fraud if PBX losses are allocated to the IXCs. The TFS believes if liability for PBX fraud is shifted to the carriers, all ratepayers, including single line residential subscribers, would be forced to contribute to the costs of this type of theft. The TFS believes it is undesirable to shift PBX theft expenses to ratepayers in general, who are not in a position to mitigate PBX fraud risks.

Finally, the Commission asks whether carriers should be required to offer services to limit customers' exposure to PBX toll theft. The Toll Fraud Subcommittee believes individual carriers should have the option to offer services to limit customer exposure. In the competitive marketplace, the customer demand for these services will stimulate the supply. However, the decision to

not offer such services is not unreasonable; IXCs vary in their size, and in their ability to provide monitoring services. Such services should not be required as part of the basic interexchange service offering.

III. PAYPHONE FRAUD.

Earlier this year, the Florida Public Service Commission asked the Commission to review interstate and international tariff provisions relating to liability for fraudulent toll calls. The Florida PSC proposed that the Commission adopt regulations mirroring regulations adopted in Florida. In the NPRM, the Commission finds merit in the FPSC's apportionment rules for payphone fraud and considers adopting this approach as a national model.

In its comments on the FPSC petition, the Toll Fraud Subcommittee stated its support for rules which place reasonable obligations upon subscribers and each industry segment. The Florida rules only apportion liability. The Commission should take steps to prevent payphone fraud from occurring. There are several specific improvements which are needed and available today.

As the Commission observes, the record in the Operator Service Access and Pay Telephone Compensation (CC Docket 91-35) proceeding showed that existing state tariffed screening services are not uniform and are frequently not available to all classes of aggregators. NPRM, fn 49. The TFS urges the Commission to require LECs to make these services available on a uniform basis. Also, the Commission should require nationwide adoption of uniform ANI

information digits for COCOT payphones, as well as for pay telephones located in correctional facilities. In addition, the FCC should encourage COCOT providers and LECs to install privacy shields surrounding payphone keypads. Such shields can reduce the ability of "shoulder surfers" to steal calling card numbers from legitimate users of the phones.

The Commission must also recognize that the Florida rules are related only to screening services which come into play in processing "0+" calls. The Florida rules do not address IXC liability in general for "1+" and 10XXX+1 calls originating from private pay telephones. This is the correct approach. The "1+" and 10XXX+1 dialing patterns are used by private pay telephones to route legitimate direct dialed traffic to the IXCs. In such cases, the COCOT owner resells "1+" toll service on a "coin sent paid" basis. IXCs are unable to distinguish legitimate "coin" traffic processed by the COCOT from traffic generated through "clip-on"[3] fraud or other manipulation of the phone itself. In at least one complaint case before the FCC involving "clip-on" fraud and 10XXX+1 calls originating from a payphone line, the payphone owner argued successfully that it was not a customer of the IXC which handled the calls and therefore could not be held liable for them. United Artists Payphone v. New York Telephone Co. and AT&T, 8 FCC Rcd. 5563 (1993). TFS disagrees with the Commission's decision to assign liability to IXCs for 10XXX+1 calls from payphones. Several

[3]"Clip-on" fraud occurs when a "clip-on" device (telephone) is attached to a line serving a subscriber (often on the carrier side of the demarcation point) and is used to make unauthorized calls.

TFS members accept 10XXX+1 dialed calls from all originating ANIs. Acceptance of these calls is consistent with the Commission's policies regarding equal access. The Toll Fraud Subcommittee believes 10XXX serves important public purposes, i.e., it promotes the subscriber's ability to use multiple carriers and to "dial around" the presubscribed "1+" carrier in cases of network blockage or failure. Allocation of fraud liability to the IXCs for 10XXX+1 creates disincentives for IXCs to accept 10XXX traffic. Private payphone owners should be required to secure their equipment and to utilize LEC services designed to inhibit "clip-on" fraud. These services should be made available by all LECs. One existing service offered by some LECs is the "PIC-None" option, which blocks "1+" interLATA calls. The NPRM implies this service is relevant to COCOT fraud prevention. ¶ 9, fn 18. However, this service is improperly characterized as a fraud control service, because "PIC-None" does not affect 10XXX+1 calls.[4]

The Commission has requested comments on whether tariffs filed by carriers for blocking and screening services should be required to clearly articulate the responsibilities of the parties and apportion the costs of fraud incurred in the use of these services. TFS is unsure how this proposal could work. LECs offer blocking and screening services to pay phone owners under tariff. IXCs do not "subscribe" to these services. Rather, IXCs receive originating line screening information as part of Feature Group D

[4]"PIC-None" in conjunction with LEC provided blocking of 10XXX+1 calls may be a way to control "clip-on" fraud.

access signalling, and receive billed number screening information in the course of querying the LIDBs. The TFS believes the LEC payphone access line tariffs can only apportion liability between the LEC issuing the tariff and the subscriber. Thus, a LEC tariff governing private payphone interconnection could not apportion liability to an IXC.

IV. "0+" FRAUD (LIDB ISSUES).

The Commission's Notice characterizes fraud problems associated with "0+" dialing and joint use calling cards as LIDB fraud. Actually, the scenarios described in this section of the Notice do not involve fraud affecting a LIDB. Rather, they involve fraudulent "0+" and "00-" calls e.g., calling card, collect, third-number billed) which occur despite the use of LIDB validation to try and prevent them. Such abuse is better characterized as "0+" fraud.

To understand the significance of the "0+" fraud problem, the Commission should first consider the importance of "0+" calling in today's telecommunications environment. The majority of "0+" fraud on IXC networks involves abuse of LEC joint use calling cards.[5] These calling cards are issued by virtually every LEC in the United States.

---

[5]LEC joint use calling cards bear account numbers supplied by a LEC, are used for the services of the LEC and a designated IXC, and are validated by access to data maintained by the LEC. Cincinnati Bell Telephone Company, 6 FCC Rcd. 3501 (1991). All TFS members accept LEC joint use calling cards and process operator-assisted calls billed to LEC line numbers.

As Judge Greene observed in 1988, "[calling cards have assumed considerable importance in consumer telecommunications, as roughly 50% of operator-assisted telephone traffic is now conducted by means of such cards." United States of America v. Western Electric Company, 698 F. Supp. 348, 350 (D.D.C. 1988).[6] LECs aggressively market these cards to their subscribers, promoting their use for completing intraLATA, interLATA and international calls. As a consequence of this promotion, IXCs desiring to participate in public telephone presubscription must accept all of these cards. It is the promotion of these cards which creates the demand for LIDB validation services.

Only a LEC can provide validation information for cards and line numbers it issues. In addition, LECs offering "0+" calling cards have a virtual monopoly on billing and collection for calls made with the cards. LECs also derive substantial access revenue for interLATA calls made with the cards, and from validation charges imposed on their LIDB customers.[7] However, when fraudulent calls are made on IXC networks with joint use cards, the financial consequences rest with the IXCs. Thus, fraudulent calling card

---

[6]The Commission, recognizing the considerable importance of "0+" calling cards, concluded in the Cincinnati Bell proceeding that the generation and maintenance of validation information for LEC joint use cards is an inevitable byproduct of the LECs' common carrier operations. The Commission's findings also apply to screening data for collect and third party calls.

[7]The TFS recognizes that not all LECs are LIDB providers; many independent LECs store validation information in LIDBs owned and administered by other parties. However, to the Toll Fraud Subcommittee's knowledge, all domestic LIDBs except one are LEC-owned.

charges create uncollectibles for IXCs, while producing collectible access, validation and billing revenues for the card issuers and LIDB providers. For international calls, IXCs also must make substantial settlement payments to foreign PTTs. The TFS believes there are no significant economic consequences today for LEC failures to properly administer their LIDBs.

All TFS members use the various LIDBs, either through direct interconnection or through gateways provided by other parties, such as Card*Tel. Importantly, all TFS members have experienced frustration with high volumes of fraudulent calling which occur in spite of systematic use of LIDB. These problems have included:

1. Failure of some LIDB providers to provide monitoring and administrative services 7 days a week, 24 hours a day — TFS members have identified instances where LECs were unable to deactivate calling cards due to understaffing;
2. Reluctance to accept fraud referrals. One BOC LIDB provider would not accept fraud referrals from a TFS member unless the member executed an indemnity agreement;
3. Failure to provide feedback in response to specific IXC fraud referrals — the lack of response makes it difficult to determine whether action has been taken;
4. Failure to act after fraud referrals. In one situation, after a TFS member identified simultaneous international calls originating from two cities and billed to the same calling card number, the LIDB provider failed to deactivate the calling card. This TFS member provides

the calling and called number on all LIDB queries;

5. Issuance of calling cards with special thresholds which permit exceptionally high use. If these cards are compromised, IXCs are at risk because the IXC has no way to know that high thresholds prevent the card from being deactivated.

The inadequacies of certain LIDBs are clearly manifested in post-billing adjustments initiated by the LECs. TFS members have found that LECs often issue billing adjustments making it impossible to collect charges for calls which were validated prior to call completion. The TFS believes some of these adjustments occur as a result of screening features being applied to an account long after billable calls have occurred.

The Toll Fraud Subcommittee urges the Commission to take steps which will encourage the LIDB providers to improve existing fraud control features in LIDB and to develop new ones. A number of solutions are offered below.

The first thing the Commission should do is find that LIDB providers are responsible for the consequences of poor LIDB administration. Importantly, as the Commission observed in the LIDB access tariff investigation, "the LECs are uniquely in control of the accuracy in the LIDB database. Moreover, the evaluation of the credit worthiness of an end user and prevention of fraud are at the very heart of why a customer orders LIDB service." Local Exchange Carrier Line Information Data Base, CC Docket 92-24, (FCC 93-400), 8 FCC Rcd. 7130 (1993). The LIDB providers should have a

stake in the performance of the databases.

In response to requests to assign such liability to LIDB providers, the LECs typically respond that they should not be required to guarantee collection of IXC revenue. However, the TFS believes allocation of liability to the LIDB provider would not merely shift the expense of fraudulent calling. Rather, it would force the LIDB providers and LECs to become more aggressive in monitoring card usage and deactivating abused cards. The same may be said of fraudulent collect and third number calls billed to numbers without billed number screening. The LIDB providers must have a financial incentive to police "0+" calls billed to subscriber line numbers. Allocation of liability will not only improve LIDB administration, it may also lead to improved guidelines for LEC calling card issuance. The issuer of a calling card is in the best position to evaluate any request for service and to determine whether to issue a calling card. A LEC has the option to provide local service to a subscriber without issuing a calling card.

The LECs also state that since they use their own LIDBs for intraLATA toll, they have adequate incentives to properly administer their LIDBs. However, the vast majority of fraud expense and lost toll revenue is for interLATA and international calls carried by IXCs.

The Commission also asks whether IXC's should be required to provide the originating and terminating number to the LECs in order

for the LECs to set fraud parameters because the LECs claim they have no tools other than velocity checks to monitor for card fraud. A proper incentive for improvement of LIDB performance is assumption of liability for the product that LIDB owners control. The LECs argue that they require this information to detect fraud. The TFS believes the same purpose would be achieved by delivering the originating and terminating NPA-NXX rather than the complete telephone number. If LIDB users are required to deliver both the calling and called number, the commission should restrict the LECs from using this information for marketing purposes.

In the NPRM, the Commission asks whether carriers should be permitted to charge for the provision of calling/called number information as part of the LIDB query. Inasmuch as an IXC provides economic benefits to the LEC by accepting its joint use calling cards, the IXCs should be able to charge for this information.[8]

At ¶ 39 of the Notice, the Commission states that "assignment of liability for toll fraud losses among LIDB providers and LIDB customers" may not lend itself to a general rule. Nonetheless, the Commission emphasizes that "LIDB providers must have incentives to make LIDB as effective as it can be" in helping to minimize the risk of toll fraud. The TFS agrees and believes that LIDB providers should not be allowed to exempt themselves from the risk of "0+" fraud.

---

[8]If LIDB providers are willing to assume some responsibility for validated fraudulent calls when associated LIDB queries included the originating and terminating NPA-NXX, LIDB users would have an incentive to provide this information without charge.

V. OTHER ISSUES.

The TFS believes the Commission should consider the need for solutions to several fraud problems not identified in the NPRM. Among these problems are subscription fraud and abuse of LEC service options like call forwarding, remote call forwarding and three way calling. These problems are discussed below.

A. Subscription Fraud.

Consistent with the concept of universal service, obtaining telephone service in the United States is relatively easy. Unfortunately, abusers understand the value of a telephone number as a "credit" or billing device. Used as such, a telephone number often serves as the key to an interexchange carrier network. The LECs are in the best position to evaluate applicants for local service, and a position to grant or deny such requests. Essentially, the LECs are the gatekeepers for the public switched network.

The ease with which local service may be obtained leads to serious fraud problems. Abusers frequently establish local service for the express purpose of making outbound toll calls, receiving inbound collect calls, or accepting charges for third number calls, with no intention to pay for any of these services. In addition, establishment of local service typically includes a request for a joint use calling card. Deposit policies vary, but most LECs require no more than the equivalent of two months estimated charges

for local service.[9] An abuser can easily place (or sell) thousands of dollars worth of calls as soon as service is established. Subscription fraud is involved in many "call sell"[10] operations, and is frequently used by associates of prison inmates. By the time abuse is detected, the "subscriber" has abandoned the premises where service was installed.

The TFS believes a substantial amount of subscription fraud could be curtailed if LECs would observe uniform and adequate business office practices related to requests for service. Such steps should include:

1. Requiring positive identification for new subscribers, and using other authentication for subscribers with previous service;
2. Positive verification of all information obtained in the subscription process. One method of verification which has apparently been successful for cellular carriers is to mail new subscribers a "welcome" kit to the address where service has been ordered. If the kit is returned by the postal service, service is interrupted;
3. Establishment of thresholds for outbound traffic originating from new business and residential accounts; and
4. Verification of requests to add optional features (e.g.,

---

[9]In virtually all cases, deposit and credit policies are determined with reference to state utility commission regulations.

[10]"Call sell" operations are organized schemes to "sell" stolen communications services, typically international calls.

call forwarding, three way calling) on existing lines.

As another weapon to fight subscription fraud, LECs need to be given the discretion to interrupt service, without notice, for accounts where fraud is suspected. In this regard, the TFS notes that the California Public Utilities Commission has permitted Pacific Bell to implement tariff language in its general subscriber services tariff which permits the telephone company to refuse or discontinue service without advance notice if the acts of the customer or the conditions upon their premises are such as to indicate intention to defraud the telephone company. This discretion extends to fraudulently placed collect and third number billed calls and to acts of providing false credit information to establish an account.

B. Call Forwarding Fraud.

As the Commission observes in ¶ 5 of the NPRM, new technologies offering the most convenience are also the most likely to present fraud opportunities. Call forwarding is such a service. While there are legitimate applications for this service, its availability makes abuse astonishingly easy. In some cases, a local telephone number is obtained for use solely in conjunction with a LEC call forwarding service. In these cases, service is sometimes established without a line installation and the call forwarding is programmable on a remote basis. In most instances, the application of call forwarding is transparent to an IXC's network. The TFS believes the LECs should be required to develop signalling protocols so that IXCs may be apprised of activated call

forwarding on subscriber lines.[11] With such information, IXCs can implement appropriate fraud controls.

C. Three Way Calling.

There are many legitimate applications for three way calling. However, three way calling is often found to be used in conjunction with subscription fraud and call forwarding fraud. There are some situations in which an IXC would apply special handling procedures for calls completed to a number equipped with central office-based three way calling. The TFS believes it appropriate for LECs to make available to IXCs information concerning the existence of three way calling on subscriber lines. The TFS is aware of one major LEC which has invested in a three-way calling fraud detection tool employed in its local network. TFS applauds this type of LEC initiative.

---

[11]The TFS is concerned that some LECs have provisioned their call forwarding services in a manner which is inconsistent with Bellcore's Local Switching System Generic Requirements for call forwarding. The Bellcore specification (TR-TSY-000217) suggests the use of an error announcement for attempts to forward a subscriber line to numbers that are code restricted or toll restricted. Adherence to this existing guideline could mitigate certain fraud problems.

D. Central Office Software Changes.

TFS is also aware of one other type of fraud problem not identified in the NPRM. TFS members are aware of certain situations where LECs' central office software upgrades have inadvertently caused failure of certain screening services and network based features designed to prevent call re-origination. In cases where a carrier installs software which creates a fraud vulnerability, the carrier should be primarily liable for resulting fraud and abuse.

VI. CONCLUSION.

The Toll Fraud Subcommittee believes there can be comprehensive solutions for toll fraud and abuse problems. In order to accelerate technical solutions to fraud, the Commission should establish rules which allocate responsibility for toll theft to the party in the best position to prevent it. Prevention of CPE manipulation should be the responsibility of the CPE owner. In the case of "0+" calling card fraud and fraud related to LEC optional services, the LIDB providers and LECs should be responsible for assuring service integrity for LIDB and other services. In the case of fraud related to IXC calling cards and authorization codes, IXCs are principally responsible for detecting and preventing fraud.

Respectfully submitted,

THE INTEREXCHANGE CARRIER INDUSTRY
COMMITTEE TOLL FRAUD SUBCOMMITTEE

By: _____

David P. Jordan
Richard J. Petillo
Co-Chairmen

DATED: January 14, 1994

Comments Prepared By: Douglas F. Brent
9300 Shelbyville Road
Suite 700
Louisville, Kentucky 40222